



aurigin

Document Summary

New
Search

Help

[Preview Claims](#)[Preview Full Text](#)[Preview Full Image](#)

Email Link: A small icon of an envelope, representing an email link.

Document ID: JP 2000-089666 A2**Title:** ENCODING/DECODING DEVICE**Assignee:** NIPPON TELEGR & TELEPH CORP**Inventor:** SUGITA MAKOTO**US Class:****Int'l Class:** G09C 1/00 A; H04L 9/06 B**Issue Date:** 03/31/2000**Filing Date:** 09/16/1998**Abstract:**

PROBLEM TO BE SOLVED: To achieve an encoding/decoding device capable of ensuring guarantee of higher safety than a conventional one.

SOLUTION: In an encoding/decoding device which encodes and decodes data at every block of a constant bit length by plural steps of encoding processing using a common secret key to the decoding and encoding, an encoding function part for realizing an encoding function is configured of non-linear processing parts 301-1-301-4 executing the disturbing calculations by using a common key created from a secret key for an inputted data and outputting the calculation results, and linear processing parts 302-1-302-3 inputting the data outputted from the non-linear processing parts and executing predetermined linear calculations and outputting the calculation results, with the 4 steps of the non-linear processing parts and the 3 steps of the linear processing parts alternately cascaded.

(C)2000,JPO

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2000-89666

(P2000-89666A)

(43) 公開日 平成12年3月31日 (2000.3.31)

(51) Int.Cl. ⁷	識別記号	F I	フォーマット (参考)
G 0 9 C 1/00	6 1 0	G 0 9 C 1/00	6 1 0 A 5 J 1 0 4
H 0 4 L 9/06		H 0 4 L 9/00	6 1 1 A

審査請求 未請求 請求項の数 1 O L (全 7 頁)

(21) 出願番号 特願平10-262073

(22) 出願日 平成10年9月16日 (1998.9.16)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 杉田 誠

東京都新宿区西新宿三丁目19番2号 日本

電信電話株式会社内

(74) 代理人 100064908

弁理士 志賀 正武

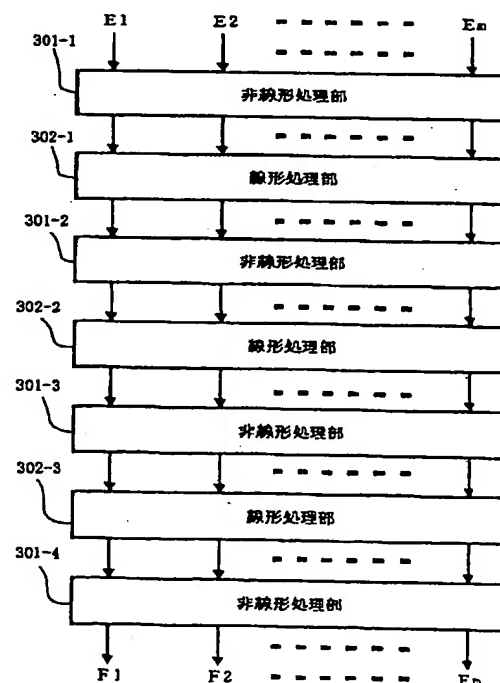
Fターム (参考) 5J104 AA01 JA10 NA08

(54) 【発明の名称】 暗号化／復号化装置

(57) 【要約】

【課題】 従来に比べより高い安全性の保証が可能な暗号化／復号化装置を実現する。

【解決手段】 復号化および暗号化に共通の秘密鍵を用い、複数段の暗号化処理段によって、一定のビット長のブロック毎にデータの暗号化および復号化を行う暗号化／復号化装置において、複数段の暗号化処理段において暗号化関数を実現する暗号化関数部が、入力されたデータに対して秘密鍵から生成された鍵を用いて攪乱演算を行って演算結果を出力する非線形処理部 301-1～301-4 と、非線形処理部から出力されたデータを入力し、所定の線形演算を行って演算結果を出力する線形処理部 302-1～302-3 とを、交互に、非線形処理部を4段と、線形処理部を3段、縦段接続して構成されている。



3

4ビットの秘密鍵から生成されたそれぞれ異なる16個の48ビットの鍵が使用されるようになっている。

【0006】図8に、図2に示す暗号化関数部202-iの他の従来の構成例を示す。図8は、NTT（日本電信電話株式会社）によって開発された128ビットブロックアルゴリズムを採用した「E2」という共通鍵暗号アルゴリズム（以下、従来技術2と称する）における暗号化関数部の構成を示すブロック図である。図8に示す暗号化関数部202-iでは、入力された64ビットのデータ Q_{i-1} が各8ビットのデータ x_1, x_2, \dots, x_8 に分割された後、非線形処理部901へ入力される。非線形処理部901では、入力されたデータ x_1, x_2, \dots, x_8 が、8個のXOR回路によって128ビットの秘密鍵から生成された第1の鍵 $K(1)$ とXORされて、その演算の結果が8個のSボックスへそれぞれ入力される。8個のSボックスでは、予め定められた置換表を参照することで入力データに対して置換処理が行われ、各8ビットのデータ z_1, z_2, \dots, z_8 が出力される。ここで、非線形処理部901では、Sボックスというデータ置換部において置換処理を行うことで、出力として、入力データに対して非線形な変換処理を行ったデータが得られることになる。

【0007】非線形処理部901から出力されたデータ z_1, z_2, \dots, z_8 に対しては、データ変換層902において下式で示す線形演算処理が行われる。

【数1】

$$\begin{pmatrix} z'_1 \\ z'_2 \\ z'_3 \\ z'_4 \\ z'_5 \\ z'_6 \\ z'_7 \\ z'_8 \end{pmatrix} = P \begin{pmatrix} z_1 \\ z_2 \\ z_3 \\ z_4 \\ z_5 \\ z_6 \\ z_7 \\ z_8 \end{pmatrix}$$

ここで行列Pは

$$P = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

【0008】なお、図8に示すデータ変換層902は、16個のXOR回路から構成されているが、これは上式を実現する一例であって、内部の構成については限定されない。

【0009】データ変換層902から出力された各8ビットのデータ z'_1, z'_2, \dots, z'_8 は、非線形処理部903へ入力される。非線形処理部903では、非線形処理部901と同様にして、8個のXOR回路を用いて入力データ z'_1, z'_2, \dots, z'_8 と秘密鍵から生成された第2の鍵 $K(2)$ とでXORを行い、さらに8個のSボックスで予め定めた置換表を参照することで置換処理を行い、処理結果として各8ビットのデータ y_1, y_2, \dots, y_8 を出力する。

【0010】非線形処理部903から出力された各8ビットのデータ y_1, y_2, \dots, y_8 には、さらに8ビットを単位とする左回転処理が行われる。そして回転処理の結果が暗号化関数の処理結果 R_i として出力される。

【0011】なお、アルゴリズム「E2」では、図1に示す暗号化／復号化装置が12段の暗号化／復号化処理段を有して構成されている。暗号化／復号化装置の全体の構成としては、図1の構成に対して、入力段と出力段に、それぞれ初期変換処理と最終変換処理を行うブロックが追加されている。また、各暗号化処理段では1つの

7
 ～401-mは、並列して動作する。各kビットの鍵K1, K1, ..., Kmは、従来の場合と同様にして1つの秘密鍵から置換、ビットシフト等の処理によって予め生成しておく。なお、非線形処理部において用いる鍵K1, K2, ..., Kmは、図1の各暗号化処理段101-1～101-j毎に異なる値とすることが望ましい。また、各暗号化処理段内で、あるいは各非線形処理部内で、鍵K1, K2, ..., Kmを同一の値にすることも可能である。

10
 【0021】図5は、図4に示す非線形処理部の内部構成のより具体的な構成を示すブロック図である。図5に示す非線形処理部は、各nビットの入力C1, C2, ..., Cmをそれぞれ入力して、入力データと同じビット長の各nビットの鍵K1, K2, ..., Kmとビット毎のXORをとるXOR回路501-1, 501-2, ..., 501-mと、各XOR回路501-1, 501-2, ..., 501-mの出力に対して、所定の置換表による置換処理を行うことでデータに対して攪乱演算を行う置換部502-1, 502-2, ..., 502-mから構成されている。置換部502-1, 502-2, ..., 502-mは、図7～図8を参照して説明した従来の構成におけるSボックスと同様の構成を用いることができる。置換部502-1, 502-2, ..., 502-mからは、それぞれnビットのデータD1, D2, ..., Dmが出力されて、後続する線形処理部へと入力されるか、または最最終段であれば暗号化関数部の出力となる。

20
 【0022】図6に図3に示す線形処理部302-1～302-3の具体的な構成を示す。図6においては行列Aの値を例えば下式のように予め定め、各線形処理部302-1～302-3の入力となる各nビットのデータG1, G2, ..., Gmに線形作用させる線形変換を定めている。図6に示す構成では、入力データG1～Gmと、行列Aから、各nビットの出力H1, H2, ..., Hmを下式のようにして求める。ただし、下式は、平文S又は暗号化文Tのブロック長を128ビット、ブロックの分割数mを8、各データG1, G2, ..., GmおよびH1, H2, ..., Hmのビット数を8ビットとする場合の例である。

【数2】

$$\begin{pmatrix} H_1 \\ H_2 \\ H_3 \\ \vdots \\ H_m \end{pmatrix} = A \begin{pmatrix} G_1 \\ G_2 \\ G_3 \\ \vdots \\ G_m \end{pmatrix}$$

ここで行列Aは

$$A = \begin{pmatrix} 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 0 & 1 & 1 & 0 & 1 & 1 \\ 1 & 1 & 1 & 0 & 1 & 1 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}$$

30
 【0023】なお、本発明による暗号化／復号化装置は、論理回路によるハードウェアによって実現することもできるし、計算機とその計算機で実行される暗号化／復号化プログラムとの組み合わせによって実現することも可能である。また、暗号化／復号化プログラムは、計算機読み取り可能な記録媒体に記録して、あるいはネットワークを介して頒布することが可能である。

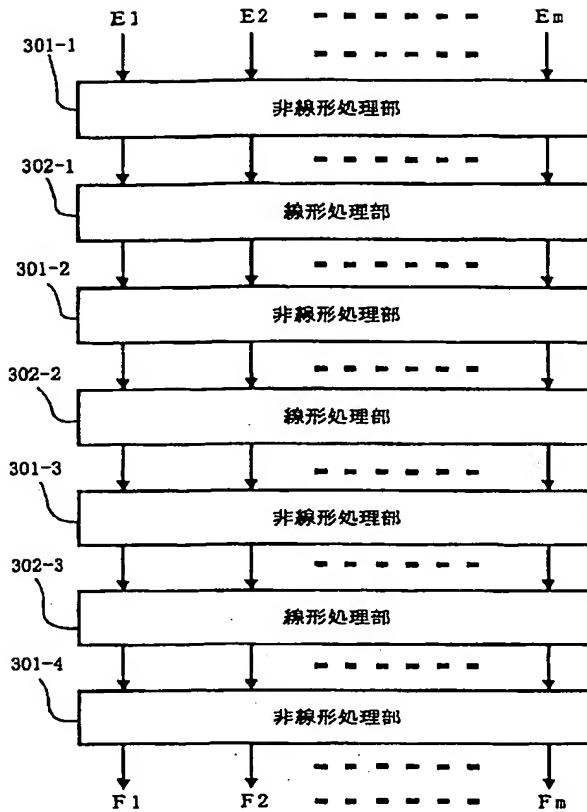
【0024】

40
 【実施例】上記発明の実施の形態において最大平均差分確率という安全性評価尺度においてj=8の場合に実際に計算することにより各置換の最大平均差分確率をpと定めたとき、暗号化関数部が2p⁸という理論的最良値(p⁸)に近い値を示し、暗号全体として8p²⁴という高い安全性が保証可能であることが確認された。これは従来技術1、2の場合と比べて高い安全性が保証可能であることを示している。

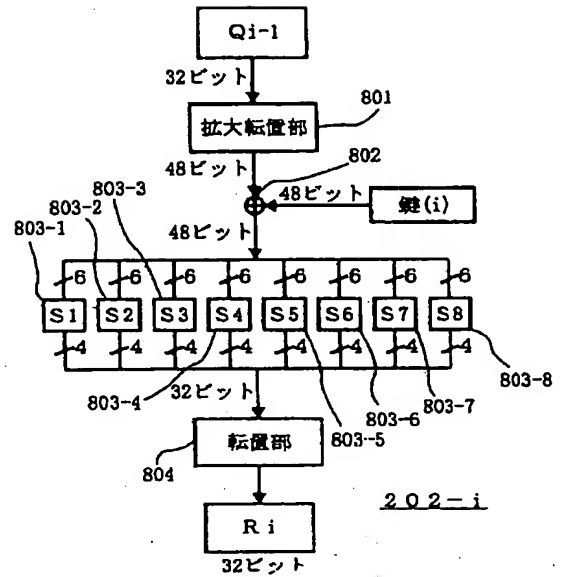
【0025】

50
 【発明の効果】本発明によれば、4段の非線形処理部と3段の線形処理部を交互に接続してなる暗号化関数部を用いて暗号化処理手段を構成することによって、従来技術に比べ非常に高い安全性の保証が可能な暗号化／復号化装置を実現することが可能になる。

【図 3】



【図 7】



【図 8】

